Lucca - Politique de Sécurité des Systèmes d'Information (PSSI)

23 Juillet 2024

Lucca - Société par Actions Simplifiée au capital de 56 519 €
Siège social : 151-157 avenue de France - 75013 Paris - France
R.C.S. Paris 441 637 691

Table des matières

1. Présentation de l'infrastructure de Lucca **4**
1.1. Contexte 4
1.2. Hébergement 4
1.2.1. Zone Europe 4
1.2.2. Zone Suisse 5
1.3. Infrastructures Lucca 6
1.3.1. Type d'infrastructure 6
1.3.2. Les protocoles de communication 7
1.3.3. Surveillance de la disponibilité des serveurs 7
1.3.4. Isolation des clients 8
1.3.5. Chaîne de sécurité 9
1.4. Prestataires et sous-traitance 9
1.5. Partenaires 11
2. Mesures de sécurité plateforme **12**
2.1. Analyse des risques 12
2.2. Risques 12
2.2.1. Coupure réseau ou électrique 12
2.2.2. Incident sur un disque 13
2.2.3. Incident sur un HOST 13
2.2.4. Sinistre majeur et PRA 13
2.3. PRA 13
2.3.1. Zone Europe 13
2.3.2. Zone Suisse 14
2.4. Gestion des sauvegardes 15
2.4.1. Zone Europe 15
2.4.2. Zone Suisse 16
2.5. Service Level Objective 17
2.5.1. Incidents Cloud-Provider 17
2.5.2. Incidents de sécurité 18
2.6. Sécurité des données 18
2.6.1. Chiffrement en transit 18
2.6.2. Chiffrement au repos 20
2.6.3. Chiffrement interne 21
2.7. Traçabilité et journalisation 21
2.7.1. Traçabilité applicative 21
2.7.2. Traçabilité interne 21

2.7.3. Traçabilité système 21
2.8. Données à caractère personnel 22
2.9. Cookies 22
2.10. Anonymisation 22
2.11. Gestion des mises à jour de sécurité 23
2.12. Antivirus et EDR 23
3. Mesures de sécurité internes 24
3.1. Gestion du parc interne 24
3.2. Politique d'authentification et de mots de passe 24
3.3. Revues des comptes et habilitations 24
3.4. Sécurité des ressources humaines 25
3.4.1. Processus de recrutement 25
3.4.2. Exigences vis-à-vis des salariés 25
3.5. Sécurité des développements 25
3.6. Sécurité des fournisseurs 26
4. Audits & certification 26
4.1. Audits de vulnérabilité et tests d'intrusion 26
4.2. Certification ISO 27001 27

1. Présentation de l'infrastructure de Lucca

1.1. Contexte

La société Lucca (« Lucca » dans la suite de ce document) est un éditeur indépendant de solutions multi-utilisateurs de gestion pour entreprise. Ces solutions sont proposées en mode SaaS.

Le présent document a pour objet la description des procédures permettant à Lucca d'assurer la disponibilité, l'intégrité et la confidentialité des données gérées pour le compte de ses clients.

Pour faciliter sa compréhension, voici une liste d'acronymes utilisée dans le document :

PRA : Plan de Reprise d'Activité.
SLA : Service Level Agreement (Qualité de service).
TLS : Transport Layer Security (remplaçant de SSL : Secure Sockets Layer).
FTPS : File Transfer Protocol over TLS.
SFTP : File Transfer Protocol over SSH.
HTTPS : Hyper Text Transfer Protocol over TLS.
VM : Machine Virtuelle.
SSD : solid-state drive (disque dur sur mémoire flash : extrêmement rapide et sans élément mobile).
PCC: Private Cloud (le PCC est un produit OVH) plateforme de virtualisation basée sur VMware.
VSAN: stockage disponible sur le réseau.
DMIA : Durée Maximale d'Interruption Admissible (Recovery Time Objective, RTO)
PDMA : Perte de Données Maximale Admissible (Recovery Point Objective, RPO)
MDM : Mobile Device Management, solution de gestion de parc.
EDR : Solution de sécurité pour détecter et répondre aux menaces cyber.

1.2. Hébergement

1.2.1. Zone Europe

Lucca a choisi l'hébergeur français OVH sur des critères de sécurité et de support.
Lucca héberge les données de production sur les datacenters :

- OVH Roubaix(France)
- OVH Francfort (Allemagne)

Lucca loue également un stockage hors OVH pour ses backups hors site, Scaleway , choisi sur la base de critères d'éloignement géographique et d'indépendance par rapport à l'hébergeur principal OVH. Les centres de données de Scaleway sélectionnés sont basés à Paris et Amsterdam, et le stockage est répliqué sur plusieurs zones de disponibilité indépendantes.

Les backups hors site chez Scaleway sont chiffrés en AES 256, le stockage est immuable avec une politique de rétention de 30 jours calendaires.

Les hébergeurs OVH et Scaleway n'infogèrent pas les infrastructures de Lucca, ils n'ont donc pas accès aux données de Lucca.

Les données de production des clients non domiciliés en Suisse sont hébergées exclusivement en Europe (France et Allemagne).

La liste des certifications OVH est disponible à cette adresse :
https://www.ovhcloud.com/fr/enterprise/certification-conformity/

La liste des certifications Scaleway est disponible à cette adresse :
https://www.scaleway.com/en/security-and-resilience/

1.2.2. Zone Suisse

Les données de production des clients domiciliés en Suisse sont hébergées sur des serveurs de Microsoft Azure basés en Suisse, sur les zones Switzerland North (Zurich) et West (Genève).

Lucca utilise un stockage de backups hors site situé chez Google Cloud Platform Storage, à Zurich, séparé physiquement des datacenter de Microsoft Azure situés à Zurich et Genève.

Les hébergeurs Microsoft Azure et Google Cloud Platform Storage n'infogèrent pas nos infrastructures, ils n'ont donc pas accès aux données de Lucca.

Les backups hors site chez Google Cloud Platform Storage sont chiffrés en AES 256, le stockage est immuable avec une politique de rétention de 30 jours calendaires.

Les données de production des clients domiciliés Suisses sont hébergées exclusivement en Suisse.

La liste des certifications Microsoft Azure est disponible à cette adresse :
https://learn.microsoft.com/fr-fr/azure/compliance/

La liste des certifications Google Cloud Platform Storage est disponible à cette adresse :
https://cloud.google.com/security/compliance/offerings#/regions=EMEA

1.3. Infrastructures Lucca

1.3.1. Type d'infrastructure

Zone Europe

Lucca exploite actuellement deux Private Cloud (PCC dans la suite du document) chez OVH, hébergeant 4 infrastructures. Les PCC hébergent les serveurs virtuels de production.

- **EU1** : Zone de production Roubaix (hébergeant les données client et applications Lucca) et PRA de Francfort
- **EU2** : Zone de production Francfort (hébergeant les données client et applications Lucca) et PRA de Roubaix

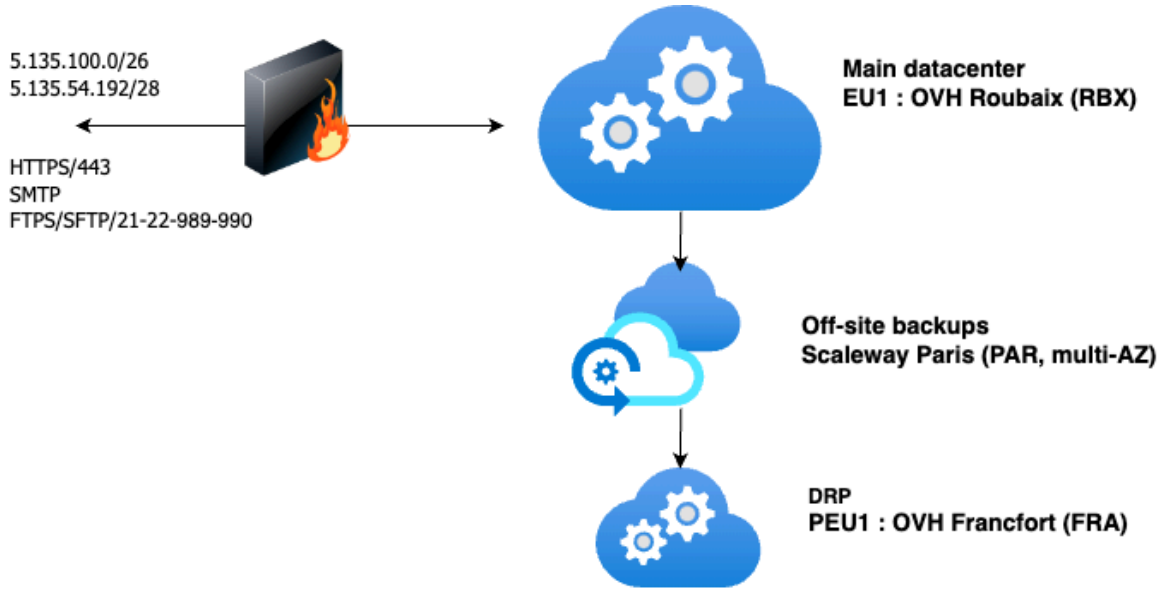
L'infrastructure Lucca est virtualisée, et utilise les OS suivants :

- Windows Server 2016/2019/2022
- Linux CentOS Stream 8
- Linux Alma 9.4

Le PCC présente toutes les redondances permettant un très grand niveau de service. Le principe de la virtualisation est l'abstraction du matériel et de ses problèmes possibles (cf §2.3). Les composants du PCC sont :

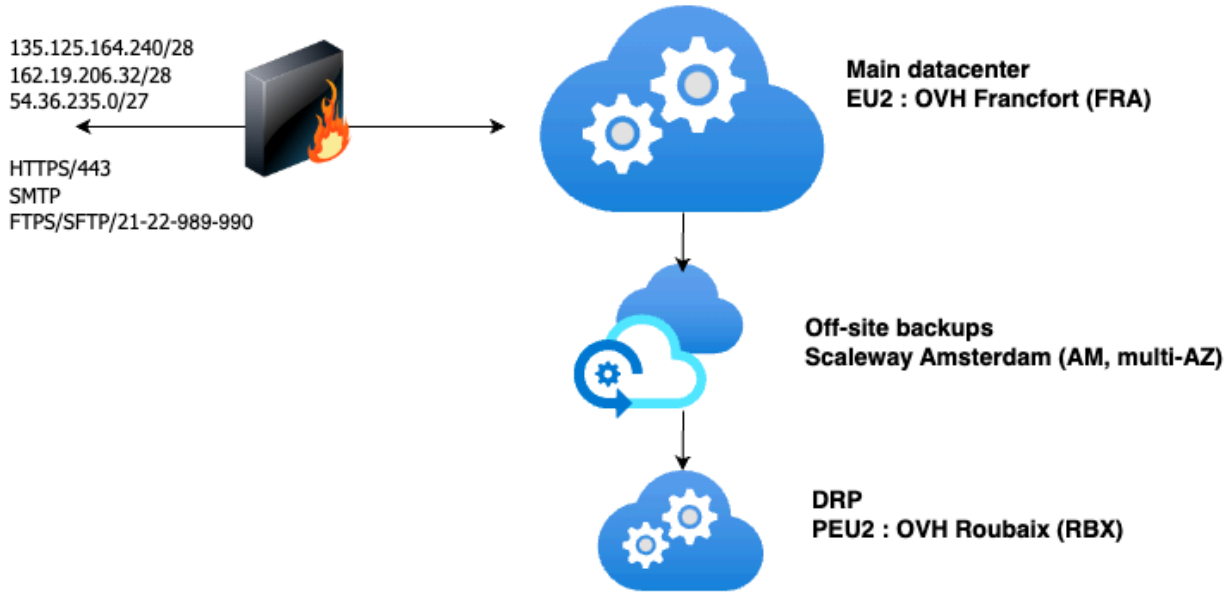
- Le **VSAN** (stockage SSD NVMe)
- Des **HOSTS** (CPU / RAM)

EU1 :



Les blocs RIPE de la Zone Europe EU1 sont : 5.135.100.0/26 et 5.135.54.192/28

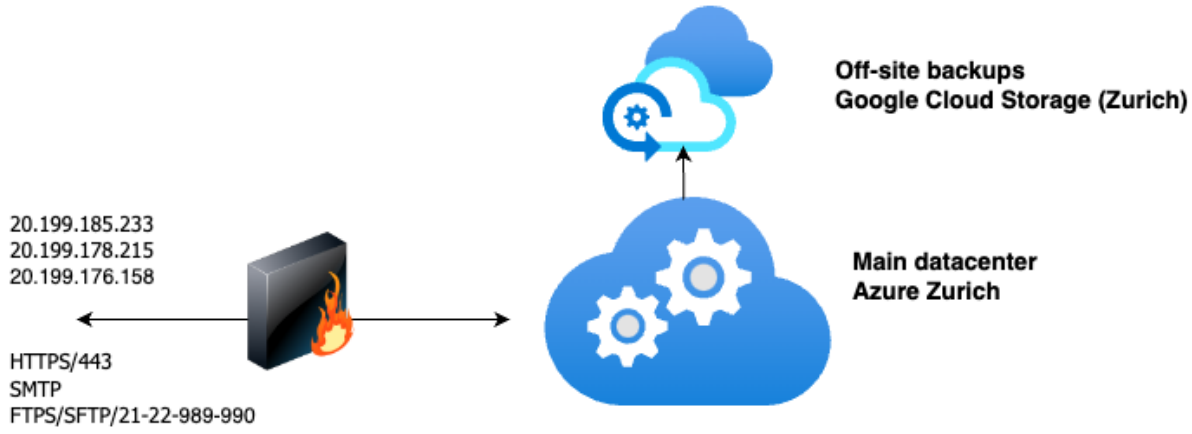
EU2 :



Les blocs RIPE de la Zone Europe EU2 sont : 135.125.164.240/28, 162.19.206.32/28 et 54.36.235.0/27

Zone Suisse

Sur Microsoft Azure, Lucca possède une infrastructure virtuelle en cloud public, sur un réseau privé.



Les IP de la Zone Suisse sont 20.199.185.233 et 20.199.178.215

1.3.2. Les protocoles de communication

Les protocoles permettant d'accéder aux serveurs ou aux données des serveurs sont limités à trois:

1. HTTPS (port 80, 443), permettant d'accéder à nos applications web à partir d'un navigateur. Seuls les protocoles TLS 1.2 et TLS 1.3 sont actuellement activés et les protocoles SSL sont désactivés. Les protocoles 1.1 et 1.0 sont désactivés depuis le 12 janvier 2018.
2. FTPS(port 990 et 989) et SFTP(port 22), permettant aux clients de déposer des fichiers sur les serveurs servant aux imports automatiques via un serveur FTP unique.
3. SMTP (port 25), utilisé en mode TLS pour l'envoi des e-mails de notifications aux utilisateurs des solutions Lucca.
   Seules les adresses e-mail hébergées par un serveur mail supportant TLS sont supportées.

Tous ces protocoles utilisent un chiffrement pour l'échange des données.

Les membres de l'équipe production de Lucca accèdent aux serveurs via un VPN et un compte nominatif avec authentification Active Directory.

1.3.3. Surveillance de la disponibilité des serveurs

La disponibilité des serveurs est contrôlée par :

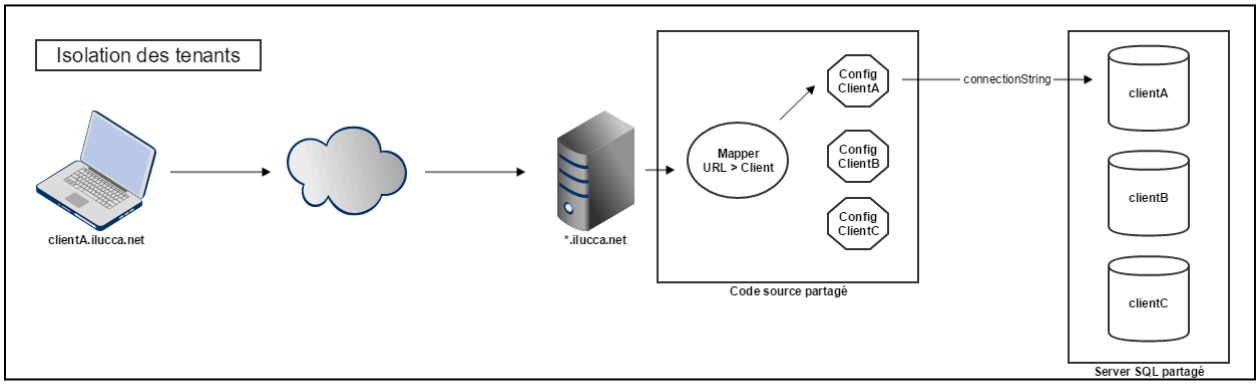
- un ping https effectué par une entreprise extérieure (internetVista) toutes les 30 minutes.
- une surveillance VMware, la technologie de virtualisation utilisée, réalisée par OVH. Cette surveillance exploite un ensemble de règles qui mesure en permanence l'utilisation des HOSTS (mémoire vive et processeur) et des machines virtuelles.
- un monitoring interne des machines virtuelles et physiques, via PRTG et Prometheus
- un monitoring avec alertes d'erreurs et de performance, via Datadog

Ces surveillances déclenchent des alertes par mail ou SMS auprès des responsables de la plateforme Lucca.

Le statut de notre infrastructure, les maintenances programmées et les incidents sont disponibles sur https://status.lucca.fr (ou tout site qui viendrait à s'y substituer) via lequel les clients peuvent s'abonner aux notifications.

1.3.4. Isolation des clients

Voici un schéma logique qui décrit le mécanisme d'isolation des données entre clients :



Les requêtes web des clients arrivent sur notre infrastructure via un serveur web frontal, qui exécute un code source partagé par tous nos clients.

Pour chaque requête, un module dédié récupère la configuration du client à partir de l'URL.

La configuration contient notamment le connectionString SQL permettant au code de se connecter à la bonne base de données.

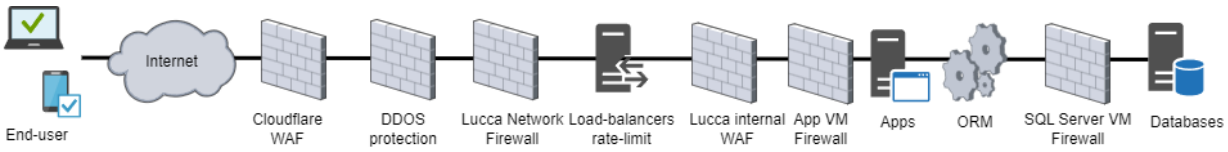
Les mesures de protection contre les attaques par injection SQL sont assurées par :

- L'utilisation systématique d'un ORM (Entity Framework)
- La présence d'un WAF, qui bloque toute tentative d'exploitation.

Toutes les requêtes utilisent un compte SQL et une base propre à chaque client.
Notre parc clients est réparti sur plusieurs "clusters" de 1 000 clients environ. Chaque cluster exploite un serveur SQL unique.

1.3.5. Chaîne de sécurité

Voici un schéma logique des différents organes de sécurité actuellement en place entre l'utilisateur final et la base de données :



- Protection WAF et anti DDOS proposées par Cloudflare.
- Protection anti DDOS proposée par OVH / Microsoft Azure
- Firewall Lucca périphérique pour l'ensemble de la plateforme + serveur VPN
- Protection rate-limit configurée au niveau de HAproxy.
    - IP bannie temporairement en cas d'attaque sur certaines URL.
    - Utilisateur bloqué temporairement en cas d'utilisation non appropriée
    - Rate-limit sur les appels d'API.
- WAF : protection applicative basée sur une liste noire
- Firewall interne, sur chaque VM
- ORM (Object-Relational Mapping) : protection contre les injections SQL
- Base de données : chaque client a sa propre authentification sur sa base de données

1.4. Prestataires et sous-traitance

Lucca a recours à des prestataires pour son fonctionnement interne.

Editeur	Nationalité	Localisation des serveurs	Activité	Lien avec Lucca	Stockage	Données personnelles

Datadog	FR/US	Union Européenne	Logs web (30j) Metrics infra (18 mois)	Toutes les solutions	oui	non
Atatus	US	US	Capteur d'erreurs client mobile	Cleemy Notes de frais	oui	non
Mindee	FR	(AWS) Irlande	OCR clients français	Cleemy Notes de frais	non (buffer)	non
Beamer	US	US	Communication interne aux applications	Toutes les solutions	non	non
Userflow	US	US	Accompagnement des clients sur les solutions Lucca via l'affichage de bulle d'aide	Toutes les solutions	non	non
Cloudflare	US	France	WAF / CDN	Toutes les solutions	non	non
Amplitude	US	(AWS) Allemagne	Statistiques d'usage des applications	Toutes les solutions	non	non

Pour les besoins de l'exécution du contrat avec le client, lorsque Lucca agit en tant que sous-traitant du client, elle a recours à des sous-traitants ultérieurs. Des données personnelles peuvent être traitées par ces derniers :

Editeur	**Nationalité**	**Localisation des serveurs**	**Activité**	**Lien avec Lucca**	**Stockage**	**Données personnelles**
OVH	FR	France	Cloud-provider	Hébergement clients UE	oui	oui (utilisateurs)
Scaleway	FR	France, Pays-Bas	Cloud-provider	Sauvegardes hors site clients UE	oui	oui, chiffrées (utilisateurs)
Microsoft Azure	US	Suisse	Cloud-provider	Hébergement clients CH	oui	oui (utilisateurs)
Azure	US	France	Cloud-provider	Poplee	oui	oui

OpenAI				Engagement - Analyse de verbatims (optionnel)		
Google Cloud Platform Storage	US	Suisse	Cloud-provider	Sauvegardes hors site clients CH	oui	oui, chiffrées (utilisateurs)
Mail OVH	FR	France	Email attachment	Cleemy Notes de frais	non (buffer)	oui (email)
Teams (Microsoft)	US	France	Workspace	Echange de fichiers	Uniquement sur demande du client en phase de lancement du projet	oui, sur demande du client
Google workspace	US	Union Européenne	Workspace	Echange de fichiers	Uniquement sur demande du client en phase de lancement du projet	oui, sur demande du client

Lorsque Lucca agit en tant que responsable de traitement, à l'égard notamment des Administrateurs du client, elle a recours à des sous-traitants. Des données personnelles peuvent être traitées par ces derniers :

Editeur	**Nationalité**	**Localisation des serveurs**	**Domaine d'activité**	**Lien avec Lucca**	**Stockage**	**Données personnelles**
Zendesk	US	Allemagne	Ticketing	Support client	oui	oui (administrateurs des clients uniquement)
Salesforce	US	France et Allemagne	CRM	Vente	oui	oui (administrateurs des clients uniquement)
Clearnox	FR	France	Recouvrement	Recouvrement	oui	oui (facturation client uniquement)

1.5. Partenaires

Lucca propose certaines fonctionnalités optionnelles, via des solutions de tiers intégrées dans les solutions Lucca. Dans ce cadre, Lucca agit en tant que simple intégrateur desdites fonctionnalités. Ces fonctionnalités ne sont accessibles par le client que sous réserve de l'acceptation des conditions d'utilisation et des politiques de traitement des données applicables. A défaut d'acceptation, le client et ses utilisateurs ne pourront avoir accès auxdites fonctionnalités optionnelles. En acceptant ces conditions, le client accepte également que Lucca communique au partenaire concerné des données personnelles figurant dans les solutions Lucca nécessaires pour le bon fonctionnement desdites fonctionnalités.

Editeur	**Solution concernée**	**Fonctionnalité concernée**
Powens (Budget Insight)	Cleemy Notes de frais	Agrégation bancaire
Swan	Cleemy Notes de frais	Ouvrir un compte de paiement au nom du client et mettre à disposition des moyens de paiement auprès des utilisateurs finaux
Universign	Cleemy Notes de frais	Archivage à valeur probante des justificatifs de notes de frais
Signaturit	Poplee Socle RH	Signature électronique

2. Mesures de sécurité plateforme

2.1. Analyse des risques

Dans le cadre de sa certification ISO 27001, Lucca a mis en place un SMSI, incluant une analyse de risque avec revue annuelle.

Ce SMSI inclut l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir et garantir la sécurité du système d'information.

Dans le cadre de la politique de sécurité, les risques envisagés concernant l'indisponibilité et l'intégrité sont les suivants :

- Coupure réseau ou électrique
- Problème sur un disque du VSAN
- Problème sur un HOST
- Sinistre majeur sur le PCC

Les risques envisagés concernant la confidentialité sont les suivants :

- Vol des données sur le réseau internet
- Vol des données sur le serveur de production

- Vol des données sur le serveur de sauvegarde
- Vol des données sur le serveur de sauvegarde hors cloud provider
- Vol des données par les salariés Lucca ou les partenaires

2.2. Risques

Les menaces identifiées sur les données gérées par Lucca sont évaluées sur les critères suivants :

1. **Indisponibilité** : masquer les données aux personnes qui doivent y avoir accès
2. **Intégrité** : altération ou destruction des données
3. **Confidentialité** : révéler les données à des tiers qui ne doivent pas en avoir connaissance
4. **Traçabilité** : être capable de retrouver qui a fait quoi et quand

2.2.1. Coupure réseau ou électrique

L'installation électrique est redondée et les fournisseurs d'infrastructures (OVH et Microsoft Azure) disposent de plusieurs groupes électrogènes et de batteries permettant d'assurer la continuité de l'alimentation électrique. L'installation réseau est aussi redondée et chaque serveur dédié a accès à deux switchs réseau. De plus, ces fournisseurs d'infrastructures possèdent plusieurs contrats d'accès à internet.

OVH et Microsoft Azure disposent d'un plan de continuité sur les domaines d'alimentation réseau et électrique.

2.2.2. Incident sur un disque

Le PCC d'OVH propose un stockage VSAN des données (configurations possibles : RAID-1, RAID-5, RAID-6).
Le SLA OVH annonce une disponibilité à 99,95% (à février 2023). La redondance du stockage sur plusieurs hosts permet de résister à l'indisponibilité totale d'un ou plusieurs host, sans aucune interruption d'accès aux données.

2.2.3. Incident sur un HOST

La protection HA (High Availability) est activée. En cas de défaillance d'un HOST, les machines virtuelles sont redémarrées sur un autre host. Le host défaillant est alors remplacé par OVH dans un délai de 15 minutes.

La continuité de service est assurée avec une interruption de moins de 2 minutes sans perte de données.

2.2.4. Sinistre majeur et PRA

Les hébergeurs OVH et Microsoft Azure disposent de plusieurs centres de données. Si celui qui héberge le datacenter principal venait à disparaître (incendie, crash d'un avion, inondation…), Lucca dispose de deux PRA (Plan de Reprise d'Activité) : un sur site et un hors site (détails ci-dessous).

Le PRA est déclenché après certitude de non-récupération des services (plateforme) sous 8 Heures Ouvrées.

2.3. PRA

2.3.1. Zone Europe

PRA sur site :
Les données sur les régions PRA (OVH PEU1 et PEU2) sont testées chaque jour automatiquement :

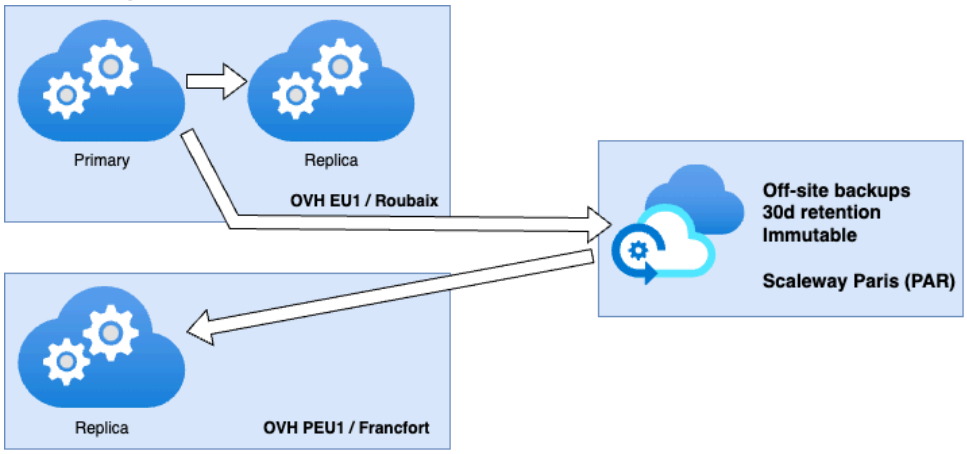
- L'ensemble des bases des clients sont restaurées, leur intégrité est vérifiée.
- L'ensemble des fichiers (justificatifs, documents…) sont synchronisés.
- L'infrastructure est minimale : seules les VM hébergeant de la donnée sont existantes. Les VM sans état (stateless) doivent être reconstruites via Ansible en cas de déclenchement du PRA.

PRA hors site :
Un deuxième hors OVH, chez Scaleway.

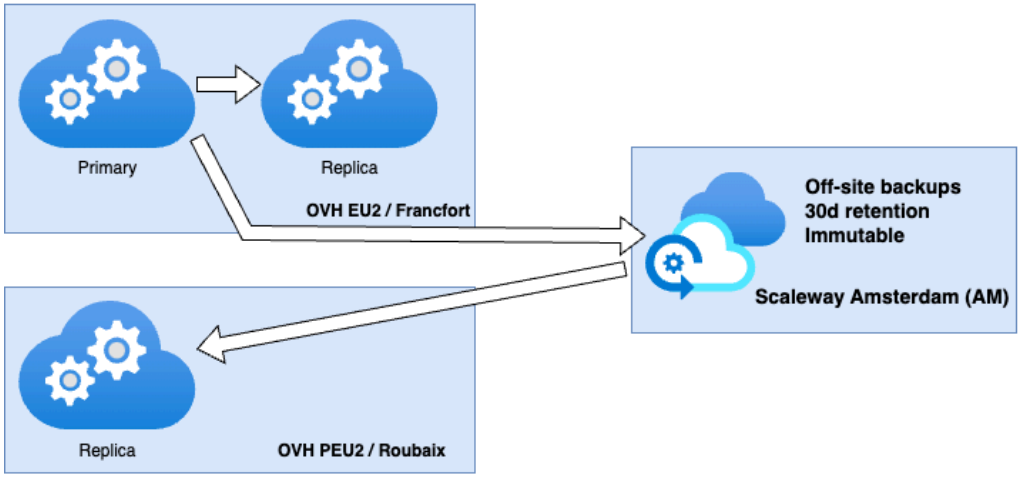
- L'ensemble des bases et fichiers sont disponibles de façon chiffrée.
- Ces archives sont transférées sur Scaleway à la fréquence du RPO.

RPO : 60 minutes.
RTO sur site : 72h
RTO hors site : 1 semaine.

Pour la région EU1 :



Pour la région EU2 :

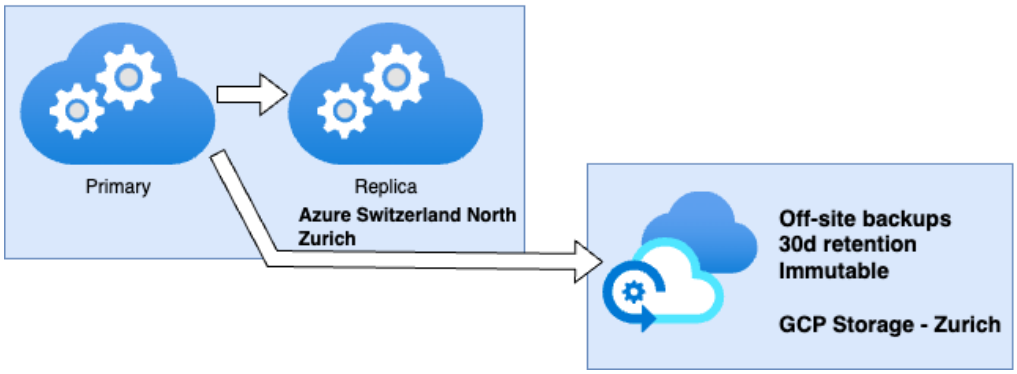


2.3.2. Zone Suisse

PRA hors site :
Les backups sont sur Google Cloud Platform Storage Zurich.

- L'ensemble des bases et fichiers sont disponibles de façon chiffrée.
- Ces archives sont transférées sur Google Cloud Platform Storage à la fréquence du RPO.

RPO : 60 minutes.
RTO sur site : 72h
RTO hors site : 1 semaine.



2.4. Gestion des sauvegardes

2.4.1. Zone Europe

Sauvegarde locale

- Une sauvegarde intégrale des bases de données est faite chaque nuit. Une sauvegarde différentielle est effectuée toutes les 60 minutes.
    - Les sauvegardes de base de données sont effectuées sur une VM séparée. Les réplicas SQL Server sont alimentés à partir des sauvegardes sur site en continu (log-shipping).
- Une réplication des fichiers est réalisée en presque-temps-réel localement, sur un second serveur. Cette redondance permet une bascule de service en cas d'indisponibilité sur serveur de fichier primaire.

Sauvegardes hors site (hors OVH, chez Scaleway)

Les sauvegardes de fichiers et bases de données sont réalisées sur site, et sont envoyées chiffrées en AES 256 sur un Object Storage Scaleway Paris / Amsterdam, dès la réalisation de celle-ci.

Le stockage des données sur Scaleway est immuable (aucune modification ou suppression des sauvegardes n'est possible, même pour les administrateurs), et avec une rétention de 30 jours. Passé cette période, les données sont automatiquement détruites. Les clés de chiffrement ne sont pas stockées sur Scaleway

Fréquence des sauvegardes hors site :

- Snapshot quotidien.
- Snapshots récurrent toutes les 60 minutes.

Sauvegardes distantes (PRA OVH)

Les données client sauvegardées sur OVH Roubaix EU1 sont remontées en continu sur l'infrastructure OVH Francfort PEU1, et respectivement les données sur EU2 Francfort sont remontées sur PEU2 Roubaix.

- Les données sont récupérées depuis le stockage hors-site de façon à valider leur intégrité.
- Les bases de données sont transférées via log-shipping.
- Les fichiers sont synchronisés en presque-temps-réel.

Les sites OVH Roubaix (France) et OVH Francfort (Allemagne) sont distants géographiquement de plus de 400 km.

La PDMA (ou RPO) est de 60 minutes pour les bases de données et pour les fichiers. L'ensemble des contextes clients sont testés automatiquement chaque jour.

2.4.2. Zone Suisse

Sauvegarde locale

De la même façon que pour la zone Europe : nous avons sur Google Cloud Platform Storage Switzerland North (Zurich) :

- Une sauvegarde intégrale des bases de données est faite chaque nuit. Une sauvegarde différentielle est effectuée toutes les 60 minutes.
    - Les sauvegardes de base de données sont effectuées sur une VM séparée. Les réplicas SQL Server sont alimentés à partir des sauvegardes sur site en continu (log-shipping).
- Une réplication des fichiers est réalisée en presque-temps-réel localement, sur un second serveur. Cette redondance permet une bascule de service en cas d'indisponibilité sur serveur de fichier primaire.

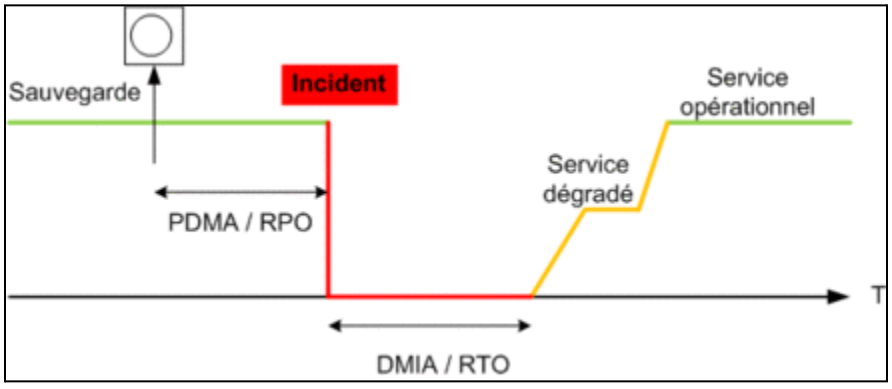
Sauvegardes hors site (hors Azure)

Pour la zone Microsoft Azure Suisse, les sauvegardes sont externalisées sur Google Cloud Platform Storage en Suisse (Zurich), et ont la même politique de rétention, d'immuabilité et de chiffrement que sur la zone France. (Rétention 30 jours calendaires).

L'ensemble des sauvegardes sont envoyées sur Google Cloud Platform Storage Suisse en temps réel, dès la réalisation de celle-ci.

Fréquence des sauvegardes hors site :

- Snapshot quotidien.
- Snapshots récurrent toutes les 60 minutes.



RTO/DMIA détaillé dans le paragraphe 2.3.

2.5. Service Level Objective

Le statut de l'infrastructure est disponible sur https://status.lucca.fr (ou tout autre site venant s'y substituer).

Le SLO global de l'infrastructure Lucca est de **99,5%**. Ce SLO est calculé hors plages de maintenance programmées, hors Incidents Cloud Provider, et hors Incidents de Sécurité (tels que définis ci-dessous).

"Heures Ouvrées" : ensemble des heures incluses dans un Jour Ouvré.

"Jours Ouvrés" : du lundi au vendredi, de 9h à 17h (heure de Paris, France), hors jours fériés en France.

"Incidents" : tout événement accidentel et/ou intentionnel qui entraîne une altération de la disponibilité, de la sécurité, de la confidentialité ou de l'intégrité des données des clients de Lucca, des solutions et/ou du système d'information de Lucca et/ou de ses sous-traitants (notamment ses cloud providers), tel que décrit dans le présent document.

"Interruption de service" : indisponibilité d'une ou plusieurs solutions de Lucca du fait d'une anomalie applicative ou d'un Incident, tel que déclaré par Lucca sur le site https://status.lucca.fr/ (ou tout autre site venant s'y substituer).

> Ne sont pas considérés comme des Interruptions de service la lenteur ou autres problèmes de performance de certaines fonctionnalités des solutions Lucca (recherches, chargement des fichiers, etc.) ainsi que les indisponibilités lors des plages de maintenance programmées et/ou les indisponibilités dues à :
>
> > (i) des problèmes liés aux applications externes ou à des tiers,
> >
> > (ii) toutes fonctionnalités, tous logiciels ou toutes solutions identifiés comme expérience pilote, version alpha ou bêta,
> >
> > (iii) des problèmes de réseaux, de connexion internet, d'API tierces et/ou de matériel ou d'équipements externes indépendants de Lucca, liés par exemple à de mauvaises tables de routage entre le fournisseur d'accès internet du client (FAI) et le serveur Lucca et/ou à problème de réseau des opérateurs téléphoniques.

2.5.1. Incidents Cloud-Provider

En cas d'Incident Cloud Provider, Lucca s'engage à faire tout son possible pour que les solutions souscrites par le client ne soient pas indisponibles du fait d'une Interruption de service pendant un laps de temps plus important que ceux définis ci-après :

Type d'incident	Indisponibilité maximum	PDMA *(perte de donnée maximale admissible)*
Perte de disque	3 Heures 40 Minutes Ouvrées	- Aucune perte de donnée si un seul disque est impacté - 1 Heure Ouvrée si tous les disques sont impactés (cf. RPO)
Corruption de données	1 Jour Ouvré	- 1 Heure Ouvrée à partir de la corruption (cf. RPO)
Panne machine physique (host)	10 minutes Ouvrées	- Aucune perte de donnée
Panne réseau (externe à Lucca)	8 Heures Ouvrées	- Aucune perte de données si pas de déclenchement du PRA - 1 Heure Ouvrée si déclenchement du PRA
Panne centre de données	15 Jours Ouvrés	- Aucune perte de données si pas de déclenchement du PRA - 1 Heure Ouvrée si déclenchement du PRA
Panne machine virtuelle (VM)	8 Heures Ouvrées par VM	- Aucune perte de données si pas de déclenchement du PRA - 1 Heure Ouvrée à partir de la corruption (cf. RPO)

2.5.2. Incidents de sécurité

En cas d'Incident de sécurité détecté sur la plateforme Lucca, Lucca s'engage à faire tout son possible pour que les solutions souscrites ne soient pas indisponibles du fait d'une interruption de service pendant un laps de temps plus important que ceux définis ci-après :

Type d'incident de sécurité	Indisponibilité maximum	PDMA *(perte de donnée maximale admissible)*
Incident de sécurité Majeur	15 Jours Ouvrés	1 Heure Ouvrée si déclenchement du PRA
Incident de sécurité Mineur	1 Jour Ouvrés	1 Heure Ouvrée si déclenchement du PRA

2.6. Sécurité des données

2.6.1. Chiffrement en transit

Les données transitent sur le réseau public dans plusieurs contextes :

- entre les postes clients et le serveur (HTTPS)
- entre nos serveurs mail et le serveur mail du client (SMTP sur TLS)
- entre les serveurs de production et les services de sauvegarde hors site (HTTPS)
- dans le contexte d'intégration via fichiers plats pour les imports / exports (SFTP, FTPS)

Dans les trois premiers cas, les données sont exploitées par un protocole sécurisé basé sur TLS, ce qui signifie que si les données venaient à être interceptées, elles seraient difficilement déchiffrables.

L'identité des domaines Lucca (FQDN) est certifiée par la société GeoTrust Inc. via des certificats de sécurité Wildcard de classe 3 (chiffrement des données via une clé de 128 bits minimum). Le chiffrement SSL utilisé chez Lucca est comparable à celui utilisé pour les transferts bancaires.

Lucca a mis en place une segmentation réseau interne (VLAN), permettant de cloisonner les environnements par niveau de risque et de criticité.

Les seuls protocoles autorisés sur les serveurs sont les suivants :

- HTTPS (et HTTP pour assurer la redirection vers HTTPS uniquement)
- FTPS et SFTP
- SMTP (TLS)

Un accès technique est possible en RDP ou SSH via tunnel VPN pour l'équipe Plateforme de Lucca.

Le TLS repose sur un certificat RSA 2048 bits (SHA256withRSA).

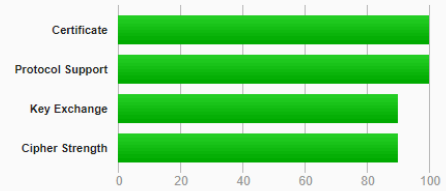
Restrictions :

- Seuls les protocoles TLS 1.2 et 1.3 sont activés.
- Les serveurs emails ne supportant pas TLS ne sont pas supportés.

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Configuration

Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Cipher Suites

# TLS 1.3 (suites in server-preferred order)	
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_SHA256 (0x1304) ECDH x25519 (eq. 3072 bits RSA) FS	128

# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3) DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f) DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128

Security Report Summary

A+

Site:	https://lucca.ilucca.net/ping
IP Address:	5.135.100.18
Report Time:	27 Jul 2021 12:50:41 UTC
Headers:	✔ X-Frame-Options ✔ Strict-Transport-Security ✔ X-Content-Type-Options ✔ Content-Security-Policy ✔ Permissions-Policy ✔ Referrer-Policy

2.6.2. Chiffrement au repos

Les données des clients sont stockées sur des serveurs de base de données (SQL Server Standard Edition). Ces bases de données sont chiffrées en AES 256 (SQL Server Transparent Data Encryption). Les données sont exposées uniquement aux serveurs applicatifs (IIS). Chaque client dispose d'une base de données dédiée.

L'intégrité des données est assurée par une redondance physique des disques (VSAN), ainsi qu'une redondance des backups (stratégie 3-2-1).

Les infrastructures de backup hors site (Scaleway pour l'Europe et Google Cloud Platform Storage pour la Suisse) ne sont utilisées que pour stocker des données qui ont été préalablement chiffrées en AES 256.

2.6.3. Chiffrement interne

Les données critiques sont actuellement chiffrées au niveau applicatif :

- Les mots de passes de nos utilisateurs sont hachés en PBKDF2 (10 000 itérations)
- Les données chiffrées de façon réversible (mots de passes FTP externes / OAuth tokens externes, etc.) le sont en :
    - AES 256 CBC
    - AES 256 GCM
    - XChaCha20/Poly1305
- Les clés de chiffrement sont uniques par application, révocables manuellement, et stockées uniquement sur nos propres serveurs.

2.7. Traçabilité et journalisation

Lucca a mis en place plusieurs systèmes d'observabilité.

- Les logs sont envoyés en temps réel sur le service Datadog EU, hors site.
- Les métriques sont envoyées sur un prometheus sur site.

2.7.1. Traçabilité applicative

Dans nos différentes solutions, une notion d'historique est implémentée pour les actions et données importantes. Ces informations sont accessibles aux clients (disposant des permissions nécessaires).

La durée de rétention de ces logs correspond à la durée du contrat.

2.7.2. Traçabilité interne

L'ensemble des accès internes aux environnements des clients à des fins de support ou de configuration est géré par une solution interne nommée Cloud Control. Cette application contient un système de journalisation très fin.

D’autre part, Lucca collecte 100% des logs d’appel HTTPS sur sa plateforme, ces logs sont envoyés en temps réel vers Datadog. Ces logs permettent des alertes temps réel sur l’infrastructure Lucca, utilisés notamment dans le cadre de la réponse à incident.

La durée de rétention est de 30 jours calendaires.

2.7.3. Traçabilité système

Sur l’infrastructure Lucca, l’ensemble des accès aux serveurs (Windows, Linux) et une partie importante des logs systèmes sont logués et envoyés (en quasi-temps réel) sur Datadog.

La durée de rétention est de 180 jours calendaires.

Ces logs sont utilisés par le SIEM Lucca pour déclencher des alertes de sécurité.

2.8. Données à caractère personnel

La protection des données à caractère personnel de nos clients est une priorité absolue pour nous.

Lors de l’accueil d’un nouveau collaborateur, une session de sensibilisation à la sécurité et à la manipulation des données personnelles est réalisée.

Tous nos contrats contiennent une clause relative à la protection des données personnelles. Un Data Processing Agreement peut être signé par les clients sur demande.

Lucca a nommé un Data Protection Officer qui peut être contacté à : rgpd@lucca.fr

2.9. Cookies

Nos applications utilisent des cookies pour servir uniquement deux objectifs :

- Maintenir une session utilisateur ouverte entre le navigateur et le serveur.
- Se souvenir de certaines préférences de l’utilisateur.

Ces cookies sont exclusivement techniques et ne traitent aucunes données à caractère personnel.

2.10. Anonymisation

Dans le cadre de la réalisation des services et notamment du support fourni par Lucca au client, Lucca accède à une copie d’environnement clients en préproduction, permettant de reproduire des anomalies remontées par des tickets support.

Ces environnements de tests internes font l’objet d’un processus d’anonymisation par défaut, à moins que les données soient nécessaires à la correction de l'anomalie.

Toutes les données ayant un impact sécurité sont automatiquement anonymisées. Ex : identifiants de sessions, adresses e-mail, fiches de paie, configuration d'authentification, etc.

Toutes les actions de restauration d'environnement, anonymisées ou non, ainsi que les accès à ces environnements sont journalisés.

Les données contenues dans les environnements de préproduction sont supprimées définitivement à la fin du contrat (aucune sauvegarde hors site n'est réalisée sur ces environnements).

Les données contenues dans les environnements de production, sont conservées pendant une durée de trente (30) jours supplémentaires suivant la date de fin du contrat ou de la solution souscrite concernée. À l'issue de ce délai de trente (30) jours, Lucca supprimera ou fera supprimer définitivement les données de la ou des solution(s) souscrite(s) concernée(s), à l'exception des données hébergées dans la solution Pagga Bulletin de paie, tel que précisé dans le contrat conclu entre Lucca et le client.

2.11. Gestion des mises à jour de sécurité

L'infrastructure est hybride. Nous avons mis en place un système d'alertes interne permettant d'être informé des différentes mises à jour de sécurité. La gestion de ces vulnérabilités se fait sur 3 niveaux :

Vulnérabilités infrastructure :

- OVH gère les mises à jour VMware VSphere.
- VM :
    - Windows : Mises à jour Windows Update hebdomadaires et automatiques
    - Linux : Mises à jour hebdomadaires

Les remédiations peuvent être réalisées manuellement dans les cas le nécessitant.
L'ensemble des vulnérabilités plateforme sont détectées à l'aide de Crowdstrike Spotlight.

Vulnérabilité IT :

L'ensemble du parc informatique est géré via MDM. Les mises à jour importantes sont automatisées sur l'ensemble du parc IT (via Microsoft Intune ou JAMF).

L'ensemble des vulnérabilités IT sont détectées à l'aide de Crowdstrike Spotlight.

Vulnérabilité code :

- La détection des vulnérabilités back et front est réalisée via Github Dependanbot. Ces vulnérabilités sont suivies et donnent lieu à la création d'incidents de sécurité à partir du niveau de criticité Majeur.
- L'analyse des dépendances de code est réalisée à l'aide d'un outil interne.

2.12. Antivirus et EDR

La protection de nos serveurs est assurée par le composant EDR (Endpoint Detection and Response) Crowdstrike Falcon, sur deux dimensions : la protection antivirale, anti malware et la détection de vulnérabilités.

Une politique de scan en temps réel est appliquée par défaut et s'applique à tous les fichiers déposés par nos clients.

Le composant EDR, configuré en mode bloquant, apporte une couche de protection supplémentaire contre les nouvelles menaces de type ransomware.

La détection des vulnérabilités est centralisée et la création d'incidents de sécurité est automatisée.

3. Mesures de sécurité internes

3.1. Gestion du parc interne

L'ensemble des collaborateurs Lucca est équipé d'ordinateurs portables, implémentant un ensemble de mesures de sécurité. Ces mesures ne sont pas désactivables et sont déployées à distance.

- Ordinateurs mis à jour régulièrement, gérés via MDM
- Blocage des stockages USB externes
- Chiffrement des disques systématique
- EDR systématique

3.2. Politique d'authentification et de mots de passe

La politique de sécurité informatique de Lucca inclus notamment :

- Favoriser l'authentification SSO
    - L'utilisation de MFA sur un service SaaS externe ou interne doit être systématique si la fonctionnalité est disponible.
    - En cas d'indisponibilité, une politique de rotation de mot de passe est mise en place. (Rotation tous les 90 jours)
- Politique de mot de passe forte
    - Interdiction de réutilisation de mots de passe
    - Chaque mot de passe est fort (minimum 12 caractères composés de chiffres, de lettres, caractères spéciaux, minuscule majuscule).

3.3. Revues des comptes et habilitations

Les processus d'onboarding et d'offboarding des collaborateurs Lucca sont gérés par l'équipe IT et visent à gérer le cycle de vie des comptes et leurs rôles.

Les événements déclencheurs de l'onboarding et l'offboarding sont issus du référentiel unique des collaborateurs : la solution Lucca Poplee Socle RH.

Le processus de revue des comptes et habilitations est quant à lui géré par l'équipe sécurité laquelle effectue une analyse semi-automatisée des éventuels écarts sur l'ensemble des silos utilisateurs Lucca, tant sur les services SaaS externes que services internes.

Ce processus garantit que seules les personnes autorisées ont accès aux ressources informatiques de Lucca et que les accès sont limités aux besoins de ces personnes.

La fréquence des revues des comptes et habilitations est a minima annuelle et au mieux de façon mensuelle.

3.4. Sécurité des ressources humaines

3.4.1. Processus de recrutement

Lucca a mis en place une vérification d'antécédents et de compétence lors du processus de recrutement comprenant notamment :

- Un test technique obligatoire selon le profil du candidat (obligatoire sur les équipes produit, développement, plateforme, sécurité, et juridique).
- La prise de référence externe selon le profil.

3.4.2. Exigences vis-à-vis des salariés

Lucca exige de ses salariés :

- La signature d'un contrat de travail incluant une clause de confidentialité.
- Le respect du règlement intérieur de Lucca, comportant une clause de confidentialité ainsi qu'une charte informatique.
- Une copie de leur dernier diplôme obtenu.
- Le niveau de formation et école du principal diplôme obtenu.
- L'année d'obtention du dernier diplôme.

Lors de l'accueil d'un nouveau collaborateur, une session de sensibilisation à la sécurité et à la manipulation des données personnelles est réalisée. Ces formations initiales sont complétées par une sensibilisation continue aux risques de sécurité.

Ces mesures visent à assurer la confidentialité des données et le respect du niveau de sécurité par les collaborateurs Lucca.

3.5. Sécurité des développements

Lucca a développé une politique interne de développement sécurisé dont le périmètre s'étend aux :

- Applications web, frontend et backend.
- Applications mobiles.
- Applications à usage interne.
- Composants de la plateforme.

Elle permet d'encadrer l'ensemble du cycle de développement, de la conception à la mise en production, en passant par les tests et la protection de l'intégration continue.

Cette politique de développement sécurisé s'appuie sur des référentiels reconnus tels que le référentiel OWASP, et les meilleures pratiques de sécurité de l'industrie. Elle vise à protéger nos applications contre les menaces actuelles et futures.

3.6. Sécurité des fournisseurs

Lucca s'efforce, dès que cela est possible, de choisir ses fournisseurs sur les critères suivants :

- Fournisseur domicilié dans l'Union Européenne ou à défaut ses services sont localisés sur un data center situé dans l'Union Européenne.
- Exigence de certification ISO 27001, SOC 2 Type 2/3, ou à défaut, évaluation par Lucca des mesures de sécurité mises en place par ce fournisseur.
- Signature d'un Data Processing Agreement dans le cas où le fournisseur traite des données à caractère personnel des clients.
- Insertion d'une clause de confidentialité dans le contrat.
- Possibilité d'audit du fournisseur par Lucca afin de réaliser une évaluation régulière de son niveau de sécurité des fournisseurs et d'assurer que les mesures de sécurité mises en place sont efficaces et conformes aux exigences de sécurité de Lucca.

4. Audits & certification

4.1. Audits de vulnérabilité et tests d'intrusion

Plusieurs audits de vulnérabilité sont effectués chaque année :

- **Audits de sécurités externes commandités par Lucca**

Ils sont effectués au moins une fois par an.

- **Programme de Bug-Bounty**

Lucca a mis en place un programme de bug-bounty privé avec la société YesWeHack.

- **Audits de sécurité externes commandités par les clients et prospects**

Ils sont réalisés plusieurs fois par an. Tout client peut réaliser un pentest après avoir contacté l'équipe sécurité Lucca (security@lucca.fr). Un environnement dédié de pentest sera provisionné et mis à disposition après signature d'un accord de confidentialité et de la délivrance d'une autorisation par Lucca.

- **Audits de sécurité internes**

Ils sont réalisés plusieurs fois par mois par l'équipe sécurité Lucca. Ces audits sont réalisés sur plusieurs axes :

  - Intégrés dans le cycle de développement sécurisé, avant mise en production de nouvelles fonctionnalités représentant un risque.
  - De façon récurrente sur l'ensemble des solutions existantes.
  - De façon récurrente sur l'infrastructure Lucca.

Un audit Qualys de notre plateforme a été mis en place et automatisé. Chaque semaine, un bilan est disponible.

Un contrôle automatique d'exposition externe a été mis en place, avec alerte automatisée.

4.2. Certification ISO 27001

Depuis le 6 Juillet 2022, Lucca est certifié ISO/IEC 27001:2013.

Le certificat est disponible à cette adresse : https://dam.luccasoftware.com/m/124f81fcb4562439/

Le domaine d'application couvre : "Les systèmes d'information utilisés dans le cadre des activités de Lucca. La sécurité des données clients traités par Lucca, conformément à la déclaration d'applicabilité (Dd'A), SMSI-FORM-06-1, Ver. 2.0 daté de 2024-06-21"

La déclaration d'applicabilité est disponible à cette adresse :
https://dam.luccasoftware.com/m/56429d82ece26cc0/